MINUTES OF THE JULY 17, 2012 MEETING OF THE DATA SECURITY AND PRIVACY COMMITTEE OF THE ILLINOIS HEALTH INFORMATION EXCHANGE AUTHORITY

The Data Security and Privacy Committee ("Committee") of the Board of Directors ("Board") of the Illinois Health Information Exchange Authority ("Authority"), pursuant to notice duly given, held a meeting at 10 a.m. on July 17, 2012 at the Thompson Center 100 West Randolph, Chicago Illinois and the Illinois State Library 300 West Second Street, Springfield, Illinois; with telephone conference call and webinar participation capabilities.

Appointed Committee Members present in person: 1. Elissa Bassler 2. Jud DeLoss 3. Carl Gunter 4. Nicholas Panomitros 5. Harry Rhodes 6. William Spence 7. David Carvalho 8. Leah Bartelt 9. Pat Merryweather	OHIT staff present: Mark Chudzinski; Krysta Heaney; Mary McGinnis; Laura Zaremba; Saro Loucks; Sonia Desai Bhagwakar; John Saran Invited Guests present: Vik Bansal; Colleen Connell; Peter Eckart; Ann Hilton Fisher; Gregory Ignatius; Marilyn Lamar; Steve Lawrence; Marvin Lindsey; David Miller; Dr. David Stumpf; Ira Thompson; Ron Warren; Karl Maurer
Appointed Committee Members present electronically: 1. David Holland 2. Tiefu Shen	Invited Guests present electronically: Mike Berry; Dr. Barry Hieb OHIT staff present electronically: Diego Estrella; Danny Kopelson; Cory Verblen
Appointed Committee Members absent: 1. Ron Isbell 2. Jennifer Creasy 3. Timothy Zoph 4. Edward Mensah	

Call to Order and Roll Call

Mr. Mark Chudzinski, Secretary of the Authority and General Counsel of the Office of Health Information Technology ("OHIT") welcomed the appointed members of the Committee present in person and electronically, and confirmed the presence of the Committee members noted above. There were no objections from the members of the Committee to the participation by electronic means of David Holland and Tiefu Shen who had advised the Secretary in advance of their attendance by electronic means necessitated by business or employment purposes.

Data Security and Privacy Committee Overview

Dr. Nicholas Panomitros, the Committee's Chairman, gave an overview of the day's agenda, explained the need for policy recommendations, and shared the Committee's work plan. Dr. Panomitros noted a change in Committee membership, indicating that Mr. Jim Anfield of Blue Cross Blue Shield resigned due to a change is his professional employment duties; Mr. Anfield was thanked for his service and dedication.

The Committee has two purposes to: 1) serve in an advisory capacity to the Board on protected health information ("PHI") privacy and security policies and 2) investigate and recommend ILHIE data privacy and security policies. With the launch of the ILHIE, the Committee was charged with developing recommendations for the adoption of privacy, security, and consent management policies. Part of these recommendations will involve removing statutory barriers with the assistance of the Illinois General Assembly. The Committee's goal is to fulfill its task of providing final recommendations to the Board by its September 19, 2012 meeting.

The purpose of today's meeting will be to hear testimony from more than two dozen stakeholders presenting on seven panels. There will be an additional day of testimony on July 27th of this year.

ILHIE Technical Infrastructure Overview

Ms. Laura Zaremba provided an overview of the architecture and implementation status of the ILHIE. Zaremba reviewed the differences between "point-to-point" or "directed" exchange and more robust query-response functionality. The ILHIE development strategy contemplates two initial phases: Phase 1 Direct messaging (uni-directional or "push" exchange) and Phase 2 aggregated data (bi-directional; query-response; or "pull" exchange).

To implement Phase 1, ILHIE partnered with a commercial Health Information Service Provider ("HISP") in December 2011. ILHIE Direct is designed to address multiple use cases and appears to be of particular utility when one or both parties to the data exchange are without an Electronic Health Record ("EHR") for example, behavioral health service providers. Zaremba provided an update of current participation in ILHIE Direct indicating that ILHIE had already exceeded its second quarter registration goals and is on track to meet its year end goal of 2,000 registrants. ILHIE Direct messaging is a first step towards a user's progression to more robust exchange of structured data between EHR systems.

Zaremba reviewed the core components of the state-wide HIE the: Master Patient Index ("MPI"), Record Locator Service ("RLS"), Provider Directory, Public Health Entity Directory, Payer Directory, data aggregation engine, and secure data transport/display. The initial ILHIE uses cases are: emergency room "pull" of aggregated PHI, clinical specialist referrals using the Provider Directory, public health reporting via the Public Health Node, and Medicaid provider incentive payment reporting.

Zaremba explained that the ILHIE is currently in test phase for bi-directional exchange, testing its MPI solution, populating the Provider Directory, and anticipates testing Public Health Node connectively in late 2012. Zaremba further explained that ILHIE is working through the on-boarding process with several alpha partners, including a Chicago-based academic medical

center, a Chicago-based Federal Qualified Health Center ("FQHC), a Regional HIE in central Illinois, and a group of small hospitals in central and southern Illinois. ILHIE anticipates alpha partners will go live in two to six months.

Ms. Zaremba's presentation can be accessed at:
http://www2.illinois.gov/gov/HIE/Documents/ILHIEupdate_DSPC071712_2.pdf

Privacy & Security Overview

Mr. Mark Chudzinski provided an overview of the patient data privacy and security implications of the ILHIE. For addressing patient concerns regarding potential misuse of patient health data, two methods of legal protection are generally proposed: 1)"misuse" laws restricting the use of PHI and 2) "gatekeeper" laws restricting the initial release of data, principally by requiring patient consent for a release.

Most patient PHI privacy laws were fashioned prior to the digital (EHR/HIE) revolution. These patient PHI privacy laws applied generally to point-to-point (unilateral directed exchange), usually involving a single point of release, a single data custodian, and a single recipient. Chudzinski explained that today's challenge is to consider how to take advantage of new health information technologies ("health IT") while accommodating stakeholder interests affected by the new technologies. Today's aggregated PHI query-response (bilateral exchange) HIEs involve multiple points of data release, multiple data custodians, and multiple recipients not all known to all parties at the time of the data release.

Chudzinski brought to the Committee's attention the Illinois Mental Health and Developmental Disabilities Confidentiality Act ("IMHDDCA"). The IMHDDCA requires patient consent with considerable specificity for release of data: it prohibits "blanket consent", it prohibits "advance consent", and it provides a durational limit on consent. The application of the IMHDDCA is unclear and arguably restricts any data aggregation query-response HIE to disclose mental health data without a new consent at the time of each data release; future data recipients are not known (at time of data creation) and date of future data release are not known.

Chudzinski noted that at the Committee's hearings on March 29, 2012, the MetroChicago HIE brought to this Committee's attention the challenge it was facing because of the IMHDDCA and the intended deposit of clinical data by participating providers in a centralized data repository. As a result, MetroChicago HIE has required of its HIE participants certain data filters: MetroChicago HIE excludes from its data repository all mental health and substance abuse data; and requires its participating providers to secure all necessary consents for the depositing in the HIE of all "Highly Confidential data", namely HIV/AIDS and genetic testing data.
In order to implement the MetroChicago HIE restrictions, OHIT understands that the flow of patient records to MetroChicago HIE is less robust that it otherwise could be and OHIT further understands that: 1) all free text data is suppressed for all patients and 2) all patient records with any mental health data are excluded. In conclusion, OHIT notes that the filtering of data by any Regional HIE or intermediaries has a potentially adverse effect upon ILHIE access to patient data.

Chudzinski's presentation can be accessed at:
http://www2.illinois.gov/gov/HIE/Documents/ILHIEupdate_DSPC071712_2.pdf

Regional HIE Technical Infrastructure Overviews

MC-HIE

Ms. Marilyn Lamar provided testimony as outside counsel on behalf of the Metropolitan Chicago Healthcare Council ("MCHC"). Lamar provided an overview of the opt-out consent approach adopted by the MetroChicago HIE. Patients can decide whether none of their health information will be available to other participants through the MetroChicago HIE – even for treatment. The consensus was that clinical care would be improved more by opt-out approach, rather than an opt-in approach because more data would be available to treating. Due to Illinois and some relevant federal laws, it was necessary for MetroChicago HIE to have exceptions to the general opt-out approach for two categories of data that require special treatment under state and/or federal law: 1) Highly Confidential PHI ("HC PHI"), generally HIV/AIDS testing or diagnosis information and genetic testing information, which requires consent under Illinois law before disclosure even for treatment purposes and 2) Excluded PHI which requires authorization or consent under Illinois or federal law. The limited scope of use permitted after consent for the second category of data makes it impractical for access through MetroChicago HIE.

With respect to the HC PHI MetroChicago HIE does not want participants sending HC PHI unless the participant, which is generally the provider, has obtained the required patient consent. With respect to Excluded PHI, due to limitations on scope of use under applicable law, MetroChicago HIE has requested participants not send Excluded PHI regardless of patient consent.

Lamar described the process by which HIE participants are collecting patient consent and the process by which those consents are recorded by and later operationalized by MetroChicago HIE. MetroChicago HIE requires HIE participant operationalize the opt-out at first visit or episode of care and optionally at subsequent visits or episodes of care. The opt-out does not expire at a specific date; the patient has to change it, if they want; the opt-out is only effective on a "going forward" basis. Lamar indicated that the patients' opt-out decision at any one MetroChicago HIE participant will be effective for all of the patient's data in the MetroChicago HIE.

Lamar shared feedback with the Committee that time and time again clinicians and others, including patients, want to maximize the amount of information in clinicians' hands. Lamar commented that granular restrictions are difficult to implement with current technology and can suppress more data than the patient requested. Lamar provided several examples, shared by MetroChicago participants, highlighting the difficulty in filtering patient records for Excluded PHI.

Lamar raised the concern of whether a new "digital divide" develops where vulnerable patients that are in mental health or alcohol/substance abuse treatment centers really are not having their important data get into HIEs. Patients with Excluded PHI are not benefiting from the technological improvements of having the data available to treating clinicians.

Lamar discussed the need for a unique patient identifier. Although part of the Health Insurance Portability and Accountability Act ("HIPAA"), implementation of a unique identifier has been

continually stalled due to privacy concerns voiced at the federal level. The ability to accurately identify patients is crucial for patient safety and critical to successful HIE implementation. Lamar explained that participants seeking data have to provide enough information to verify that they are seeing a particular patient and reduce the instances of inadvertent access. However, Lamar further explained that in some limited situations, MetroChicago HIE is setting the parameters a little more broadly to have more latitude in locating the right patient.

Lamar noted that Illinois does not have a so-called "break the glass" exception that is consistent across all statutes. Lamar advocated that the Committee consider adopting a general medical emergency exception. Lamar explained that the MetroChicago HIE does disclose to patients that if they elect to opt-out their information will not be available in an emergency situation.

Dr. Carl Gunter asked Lamar to provide additional information on how providers are identifying data to be excluded and how reliable those providers think those techniques are. Dr. Gunter inquired as to whether data sequestration techniques causes providers to, maybe exclude too much data in some cases or even fail to participate in exchange. Lamar responded that providers have had to work with their vendors to custom fashion filters; unfortunately, there is nothing quick, commercial, or inexpensive on the market.

Ms. Elissa Bassler asked if the MetroChicago HIE has any statistics on the experience of patients' decision making around opt-out. Lamar explained that MetroChicago HIE does not have any data yet. Bassler asked if MetroChicago HIE continues to collect information on individuals that have opted-out and back into the system. Lamar explained that yes, even when the patient opts-out the provider may choose to continue sending data to the MetroChicago HIE. It is the HIE that is responsible for operationalizing the consent. If the patient later decides to opt back in to the system all of their data, including the data during the period for which they have opted-out will be accessible to participating providers.

Mr. Tiefu Shen asked if in addition to improving individual patients' health and improving patient safety, is improving public health and disease monitoring within scoop for MetroChicago HIE. And if so, has MetroChicago HIE assessed the impact of patient opt-out data completeness and data quality? Lamar explained that MetroChicago is interested in linking to the State for public and population health purposes, noting however, it is likely a future use case.

Mr. William Spence asked about MetroChicago HIE's policy regarding behavioral health data for adolescents. Lamar explained that all mental health records are currently excluded, whether they are children or not.

Bassler asked about MetroChicago HIE's policy with respect to the use of the data for research. Lamar explained that all MetroChicago HIE participants were very concerned about data use for research. There are fairly long provisions in the MetroChicago HIE participation agreement precluding data for research purposes without participant consent. Lamar further explained that MetroChicago HIE will pursue adopting a policy through its Advisory Council and probably the Board of Metropolitan Chicago Healthcare Council. Bassler asked about the extent to which the agreement with participating hospitals in regard to research allowed for data use for population

health purposes. Lamar commented that the MetroChicago HIE has some broader rights to look at population health.

Ms. Lamar's presentation can be accessed at:
http://www2.illinois.gov/gov/HIE/Documents/mchc_7-17-12%20testimony%20Final.pdf

CIHIE

Mr. David Miller presented on behalf of the Central Illinois Health Information Exchange ("CIHIE"). Miller provided a status update on CIHIE's activities. CIHIE is live and participating hospitals are actively collecting patient consent and data; data will be made available for viewing after 60-90 days of data have been collected.

Miller shared with the Committee the difficultly CIHIE has encountered launching due to concerns regarding what data HIE participants can share. Consequently, the HIE services CIHIE is offering are substantially less than planned; CIHIE has had to scale back from its initial plan to generate an Aggregate Community Record.

CIHIE's vision for that Aggregate Community Record was that it would include medication lists, transcribed reports, and medical history. However, at this time, CIHIE is unable to accept any of that data from any of its participants because there is a possibility that the data could include behavioral health data, genetic testing data or any other sensitive data covered by specific protections under state and federal law. CIHIE is currently only accepting and exchanging demographic data, labs, and allergy lists.

Miller brought to the Committee's attention the functionality of Direct, noting that CIHIE recognized early on the importance of direct messaging especially in regard to the exchange of behavioral health data. CIHIE would like to see changes in the legal and regulatory environment to allow for the exchange of behavioral health data. CIHIE explained that behavioral health providers have limited view rights; it is hoped that this will allow those providers to know when their patients are at the emergency room or visiting their primary care providers and it is believed this will help those providers track, follow and manage their patient care much better. CIHIE will continue to evaluate how view only access impacts patient care and care coordination.

Miller provided an overview of the process by which CIHIE retrieves and stores data from participating providers; individual data feeds from each participant are fed into individually secured vaults. CIHIE does not consider data stored in provider specific secured vaults to have been disclosed or released; it is only ready to be disclosed or released. CIHIE would ask the Committee or State to provide more clarity as to the point of disclosure and re-disclosure.

Miller explained that CIHIE is not backfilling dates, so every piece of history not collected is a piece of history that CIHIE will not have if at some point, when the patient decides that they are ready to share their data or the legal environment is such that allows exchange of sensitive data, that CIHIE will have that data available to share.

Like the MetroChicago HIE, CIHIE is using the opt-out model. In its first three weeks CIHIE has had 60,000 individual registered in the system and only eight opt-outs, approximately one in

10,000. Miller attributed the high rate of patient participation to the fact that CIHIE is only a clinical system; CIHIE is not allowing, at this point, secondary use of the data. Miller provided an overview of the process by which HIE participants are collecting consent noting that a brochure was developed and providers have designating staff responsible answering patient inquires.

Miller explained that CIHIE is supporting an opt-out model that allows a patients to opt-out data at the provider level. A patient has the ability to opt-out all the data from a participant, an entire encounter or just a result or document. CIHIE hopes that by tracking how patients opt-out they will uncover the real source of patient privacy concerns. Currently, patients have opted-out entire participants or organizations. Miller further explained that CIHIE does not have the capability of applying a patient's opt-out at one participant from the entire HIE. CIHIE is aware this places additional burden on patients and is working diligently to appropriately educate patients; however it does provide some flexibility too by allowing patients to choose not to share data from a particular specialist while allowing all other data to be available.

CIHIE is not currently allowing break-the-glass. Miller discussed the concerns voiced by HIE participants regarding break-the-glass. Miller shared that two participating organizations were not comfortable with allowing break-the-glass for patients that had opted-out; these providers believe strongly that if a patient opts-out their data should not be available anywhere under any circumstances, especially when they do not have any direct control over the provider accessing the data.

Miller explained that CIHIE is not currently allowing secondary use of data. Miller expressed concerns voiced by CIHIE's parent organization, Quality Quest, that improving care will require secondary data use to analyze the data.

Miller concurred with MetroChicago HIE on the difficulty of achieving granular sequestration of data. Extraordinary efforts have been put in place in order to filter data and the costs are very expensive, Miller noted that most of CIHIE's initial participants have been unsuccessful. Consequently, CIHIE is only sharing demographics, lab results and allergies.

As far as patient access and error correction are concerned, CIHIE supports the idea that data correct occur only at the data source.

Dr. Gunter noted it was interesting to hear how the two Regional HIEs have implemented different policies to operationalize the same opt-out consent mode. Dr. Gunter indicated it will be import for the Committee to learn from the various implementations and how to keep from confusing patients, for example with a variety of different semantics for opt-out. Dr. Gunter asked what CIHIE thought about adopting uniform statewide processes. Miller responded that CIHIE would support uniform statewide processes and looks to the Committee to identify those processes.

Mr. Miller's presentation can be accessed at:
http://www2.illinois.gov/gov/HIE/Documents/CIHIE%20-%20%20Data%20Security%20-%20Privacy%20PublicTestimomy%20Slides.pdf

LLHIE/IHEP

Ms. Mary McGinnis provided testimony on behalf of Steve Lawrence in his role as Executive Director of Lincoln Land HIE ("LLHIE") and Illinois Health Exchange Partners ("IHEP"). An overview of both HIEs was provided, explaining that each organization has its own governing boards to allow each to respond to unique market requirements in each geography, but share technology, infrastructure, staffing, and administrative services to facilitate a shared sustainability model. LLHIE and IHEP have contracted with Medicity to provide the Medicity Novo Grid and iNexx platforms. LLHIE will be in production later this summer and ILHEP will be in production sometime late fall.

It was explained that because so many physician practices in rural communities and in the Metro-East area are largely paper-based, LLHIE and IHEP looked at how to support them with the HIE network while they transitioned to the electronic exchange environment. LLHIE and IHEP founders and stakeholders determined that electronic orders, results, and referrals were the highest priority for implementation. Health system and hospital Chief Executive Officers that participated in the building of the necessary social capital to establish and financially sustain the HIEs determined these use cases met critical business requirements and clinical needs. LLHIE and IHEP do not have plans to implement a centralized community database with a MPI or RLS as this was not a priority for founders at this time because their physicians did not want to have to seek patient information from another portal outside of the practice's EHR.

An overview of LLHIE and IHEP's privacy and security framework was provided. LLHIE and IHEP each engaged with Steve Gravely and Erin Whaley of Troutman Sanders as legal counsel because of their expertise in health information exchange and their experience working with other HIEs around the country. The policies and procedures developed by legal counsel are compliant with state and federal laws and are comprehensive in addressing legal, operational, privacy, and security matters. The policies and procedures cover workforce member confidentiality and compliance, discipline, breach notification, business associate agreements, uses and disclosures of PHI, the minimum necessary standard, accounting disclosures, security risk management, suspension and termination procedures, security awareness and training, malicious software, log-in monitoring, password management, contingency plan, data backup and disaster recovery plans, emergency mode operation plan, evaluation of security policies and procedures, facility access and security, person or entity authentication, transmission security, data integrity, and others in the comprehensive manual. In addition, each participant in the LLHIE and IHEP Network is required to sign a comprehensive participation agreement that outlines privacy and security obligations and responsibilities and acknowledges that they will abide by the policies and procedures of the both HIEs.

Mr. Lawrence's submitted written testimony can be accessed at:
http://www2.illinois.gov/gov/HIE/Documents/15_Testimony_Steve_Lawrence_Final_for_7%2017%202012.pdf

Public Testimony – Patient Choice Options and Permitted Uses for Patient Data and Granularity of Patient Data

Ms. Sonia Desai Bhagwakar gave a brief presentation on patient choice and patient data. Bhagwakar identified four key policy questions regarding patient choice under consideration by the Committee.

1. Should patients be given a choice as to whether their health data can be part of an HIE? Or is HIPAA enough?
2. If the patients are given a choice beyond HIPAA, should all patients be provided the option to affirmatively consent to HIE inclusion ("opt-in") or should their health data be included automatically unless they affirmatively decline inclusion ("opt-out")?
3. Should patients have the ability to sequester specific elements of their patient record from specific providers ("granularity") or should the entire patient record be excluded from the HIE if a patient desires some data be sequestered ("all in or all out")?
4. If someone chooses not to participate in the HIE, should their data be entirely excluded from the HIE or should it just not be visible? If a patient chooses against use of the HIE, may the data still be collected by/made accessible to the HIE for mandatory public health reporting or for emergency medical treatment ("break the glass")?

Bhagwakar provide an overview of existing federal and state law regarding patient choice. Federal HIPAA Privacy Rule requires that patient consent is given for all PHI disclosures unless it is otherwise expressly permitted; an exception exists for certain disclosures for purposes of "Treatment", "Payment" and "Healthcare Operations", (the "T-P-O" exception). Bhagwakar noted additional exceptions for public health activities, research purposes and for other legally required disclosures such as public health reporting of certain diagnosis. Illinois, like many other states, have laws that provide heightened privacy protection for certain data: mental health data, substance abuse data, HIV/AIDS data, genetic testing and other data; these statutes impose more stringent patient consent requirements.

Bhagwakar summarized the policy positions taken by several federal agencies. The U.S. Department of Health and Human Services ("HHS") Office for Civil Rights has been of the view that patient data can be transmitted through an HIE for treatment purposes without the need of a prior patient consent. HHS Centers for Medicare & Medicaid Services in 2011 issued rules regarding Accountable Care Organizations which encourage the sharing of patient data among participants using a patient "opt-out" system and that would be the case even for T-P-O purposes. Most recently, HHS Office of National Coordinator for Health Information Technology recently issued guidance that patients should be provided a "meaningful choice", either on an "opt-in" or "opt-out" basis this would be the case even for T-P-O purposes. Meaningful choice refers to a patient making a choice based on some meaningful exchange of information they receive about the HIE.

Bhagwakar provided a basic overview of the five core consent models: no-consent, opt-out, opt-

out with exceptions; opt-in, and opt-in with restrictions. Bhagwakar provided a national perspective on consent models; 27 states currently have adopted an opt-out type of model; 12 states have adopted an opt-in model; no consent is required in 3 states and 8 states are still determining the issue.

Ms. Desai Bhagwaker's presentation can be accessed at:
http://www2.illinois.gov/gov/HIE/Documents/11c_Panels%201-2%20presentation.pdf

Mr. Ira Thompson and Mr. Ron Warren of Infinite Systems Support discussed the importance of audit systems.

Thompson reviewed the HIPAA Audit and Control Security Standard, 45 CFR 164.312, and covered entity requirements under that standard. Infinite Systems Support recommends an audit framework that is standards-based and compliance-governed. Thompson described the potential adverse effects that may result from an audit system without some type of governance structure to ensure there is compliance with security standards.

Infinite Systems Support believes that a monitoring and compliance program is essential to ensuring the protection of patient information, noting that no patient will maintain trust in the system without assurance that security standard compliance is enforced. Infinite Systems Support maintained that the State has a fiduciary responsibility ensure standards are in place and enforced.

Thompson discussed the challenge of balancing patients' interest in obtaining appropriate care based on knowing all the components of their conditions and patients' interest in protecting their information access to providers. Warren raised the question of patient access to their own data noting that it is unclear what methodologies have been identified to give patients access to their data.

Mr. Thompson and Mr. Warren's testimony can be accessed at:
http://www2.illinois.gov/gov/HIE/Documents/Infinite%20Systems%20Support_Transcript_7.17.2012.pdf.

Mr. Marvin Lindsey provided testimony on behalf of the Community Behavioral Health Association ("CBHA"). Lindsey provided an overview of CBHA's association members and the services those behavioral health care organization members provide.

CBHA endorses a broad statewide health integration agenda to promote better coordinated, less fragmented care. Lindsey brought to the Committee's attention the unique needs of individuals requiring behavioral health services due to frequent use of the health care systems and a greater need to coordinate care among diverse providers.

CBHA recognizes that access to comprehensive patient health record which includes behavioral health information is important to providing quality care and achieving desirable health outcomes. CBHA views the electronic exchange of patient data and the HIE as one of the means to accomplish the desired health outcomes; but should not outweigh potential privacy and

confidentiality concerns.

CBHA recommends adopting an informed consent policy that allows patient choice and clearly informs the patient, or someone authorized to act on the behalf of the patient, the exact purpose of the use of their patient information. CBHA also encourage the development of a consent management function within the HIE that can accommodate variant consent directives.

Lindsey noted that CBHA understands that certain state and federal laws will need to be amended in order for the behavioral health community to fully participate in the HIE, either using an opt-in or an opt-out model. It is CBHA's position that the HIE patient consent policies should not be a barrier to information sharing or to the inclusion of the behavioral health community in the HIE. Lindsey identified additional patient rights with respect of patient consent and control of data noting that patients should have the choice of participation in the HIE and that patients must be assured that appropriate technology solutions, business practices, and policy protections will be employed to prevent their information from being used in undesirable ways or to infringe upon their rights and civil liberties.

CBHA recommends the sharing of behavioral health history, medications and treatment within the HIE. CBHA also recommends the development of policies that allow patients the ability to sequester their behavioral health records from specific providers that are not involved in their immediate care. Lindsey also expressed CBHA support for a break-the-glass exception and the use, by public health officials, of data strictly for the purpose of population health planning and evaluations.

Dr. Gunter asked a clarifying question regarding CBHA's position: Is CBHA advocating that the exchange supports not only sharing of the records of people who have mental health issues but the mental health records themselves. Lindsey confirmed, noting that both legal and technical issues need to be addressed to allow for the sharing of behavioral health records. CBHA understands that certain statutory changes need to be made and will probably advocate for those changes.

Mr. Lindsey's submitted written testimony can be accessed at:
http://www2.illinois.gov/gov/HIE/Documents/CBHA_Testimony%20before%20ILHIE%20Authority%20Board-%20DSP%20Committee.pdf

Ms. Ann Hilton Fisher testified on behalf of the AIDs Legal Council of Chicago ("ALCC"). The ALCC promotes strict confidentiality in order to invoke trust among patients and their providers. The key to this trust is giving patients control over their medical data.

Fisher applauded current Illinois HIV confidentiality laws as being the best in the nation. Fisher shared the importance of identifying and treating individuals with HIV as critical for reducing the community viral load and reducing generally the incidence of HIV within a community.

Without strong confidentiality, individuals will not seek testing and medical care if they fear that their information will be disclosed without their consent. Fisher highlighted the still persistent stigma and discrimination faced by individuals with HIV/AIDS. The public health purpose

behind current law is to protect patient confidentiality to encourage individuals to get tested and seek treatment. Additionally, Fisher noted that the strict treatment adherence for individuals with HIV/AIDS (for example, medications and regular lab work) requires a very close trusting relationship between the person with HIV and the provider.

Fisher stated the key to Illinois' HIV confidentiality law is that an individual has control of their medical data. Fisher spoke to the importance of informed patient choice and consent practices. It is the position of the ALCC and the AIDS Foundation of Chicago that the ILHIE adopt an opt-in consent model. Fisher went on to say that only an opt-in model where patients give affirmative consent to participation will achieve informed and meaningful patient consent. Fisher added that because of the trust relationship already in place between HIV providers and patients, it is unlikely that opt-in would present a barrier to participation.

ALCC support granular sequester of sensitive information, including HIV information. ALCC acknowledges current technical challenges to sequestrations but encourages the Committee to continue to work to resolve current barriers to granular sequestration.

Fischer noted another opportunity to consent, and perhaps the most important opportunity to consent, at that point when that information is going to be used.

Mr. Jud DeLoss asked: From a policy perspective, is it more valuable to continue to maintain HIV/AIDS information as separate to segregate it from other information, to keep it more protected and more secret than other health information? Would that in your opinion, or in your organization's opinion, limit or desensitize people to this stigma or is it better to actually treat it as the medical condition that it is?

Fisher responded that this argument has been presented. However, Fisher assured the Committee that to her knowledge, not a single case of discrimination seen by the ALCC has been caused by somebody saying "Oh, there's a special law about HIV therefore it must be a terrible disease". Fisher stated there is stigma associated with this disease because it is associated with homosexuality, with drug use, with sex workers, with a much marginalized community. The stigma absolutely exists, prevails, and the law is the result of the stigma; the stigma is not the result of the law. The stigma continues therefore the protections must continue.

Ms. Fisher's submitted written testimony can be accessed at:
http://www2.illinois.gov/gov/HIE/Documents/18_ALCC%20Illinois%20health%20exchange%20testimony%20july%202012_1_.pdf

Mr. Peter Eckhart testified on behalf of the Illinois Public Health Institute ("IPHI"). Eckart provided background information on IPHI, including their participation in the Illinois Health Information Security and Privacy Collaborative ("HISPC"), an early federal initiative to address privacy and security in the (then) upcoming world of inter-connected EHRs.

IPHI strongly favors the opt-out model of patient consent, in which all patients should be given the option to opt-out of EHRs and health information exchange systems. Eckart further clarified IPHI's position; IPHI believes that the Illinois HIE and its affiliated regional exchanges should

make patient data available through the ILHIE and among the regional exchanges as its default policy. IPHI beliefs that this creates concomitant obligations on the part of the HIE operators to secure patient data as strongly as possible, and to restrict access to this data to only those who need it for valid medical or operational reasons. The opt-out approach is important to the efficient and effective operation of the HIE. It is also critical to ensuring the highest quality of patient care; without access to medical records, physicians and other health professionals are less able to make appropriate diagnoses and treatment decisions.

Eckart explained that public health is reliant on aggregated, not individual, data for understanding what health problems are affecting which groups of people and where. Data helps public health plan population-level interventions, evaluate the efficacy of public health programs, and advocate for policies that improve the public's health. IPHI sees the Illinois HIE as a new and powerful mechanism that will improve our understanding of the health of Illinois residents and sub-groups within the population. Opt-out consent is likely to lead to the highest percentage of residents participating in the Exchange; comprehensive aggregated data is the key to better policies and healthier people. The opt-out policy of consent health information exchange will result in as comprehensive a set of data as possible.

Dr. Gunter stated that based on testimony from HIEs in Illinois and across the county some providers are wary of data being extracted from the HIE for research purposes. Do you believe there might be a risk to provider participation if the HIE allows secondary data use for research purposes? How do you propose the ILHIE overcome this issue? Eckart responded that the reticence described on the part of providers may be because it is relatively early in the process of interconnecting theses systems and working towards secondary use of this data.

Dr. Gunter asked if IPHI supports some sort of governance system that would show a pathway to public health uses of the data; even if maybe that cannot be made available immediately. Eckart responded yes, that is correct.

Dr. Gunter asked Eckart to provide additional details on the technical aspects of the public health connectivity to the HIE. Eckart spoke to the general framework for public health pull out aggregated data from the federated model and do queries that result in aggregated de-identified data.

Mr. Eckhart's submitted written testimony can be accessed at:
http://www2.illinois.gov/gov/HIE/Documents/16_IPHI%20Testimony%20to%20the%20Illinois%20Health%20Information%20Exchange%20Authority.pdf

Mr. Gregory Ignatius shared with the Committee his personal experiences as a patient with a complex medical diagnosis seeing multiple providers, the difficulties he encountered with both accessing his own records and having records appropriately shared between treating and referred providers and the impact of the care he received.

Ignatius stated that the current practice of sharing information largely uses unsecured fax lines. Current methods as unsecured fax lines do not provide the privacy patients expect, and as a result, hinder efficient and sufficient medical treatment that could potentially be life saving.

Ignatius expressed concerns that patients are expected to be responsible for information being sent to treating physicians rather that the expectation being on the physicians and system to support care coordination. Electronic exchange gives the option of sending complete records, and it can be done with encryption so it is genuinely secure.

Ignatius shared his anxiety that not having a way to exchange health care information electronically makes it almost certain that he will receive the wrong care if he ever needed to go to an emergency room. Ignatius advocated for robust electronic health information exchange. The current situation does not protect patient privacy and creates situations where health care professionals do not have adequate information to make informed clinical decisions.

DeLoss asked Ignatius about his position regarding changes to behavioral health laws to allow for the inclusion of behavioral health data in the exchange. Ignation noted a number of different mechanisms for providing segregated encryption and advocated for their use.

Mr. Ignatius's submitted written testimony can be accessed at:
http://www2.illinois.gov/gov/HIE/Documents/HIE%20Testimony_Gregory%20Ignatius.pdf

Ms. Colleen Connell, the Executive Director of the American Civil Liberties Union ("ACLU") provided the Committee with recommendations for the privacy, security, and consent management policies; particularly with respect to privacy protections and privacy concerns of patients in some of the more sensitive areas of healthcare.

The ACLU advocates for informed patient consent, in which each patient has the ability and opportunity to have an informed consent dialogue about the extent that their information might be shared and with whom. This consent should include the ability to give consent to share granular pieces of their PHI on sensitive data as genetic testing or reproductive health; and should also protect minors. Connell stated that the ACLU, as indicate in its written materials, believes that an opt-in with restrictions consent model is the mechanism that best protects patient privacy as recognized in both statutory and case law in the U.S.

Connell stated that the HIPAA Privacy Rule is insufficient to manage use of data through the ILHIE. HIPAA is a floor and not a ceiling. It recognizes this itself and it specifically permits covered entities to seek patient consent. Perhaps most importantly, HIPAA specifically incorporates limits on the sharing of information. The limitations in statute for behavioral health, HIV/AIDS, substance abuse treatment as well as other areas of sensitive PHI require devising a system that allows the patient great ability to control the granularity of their PHI that is available for sharing on an electronic exchange and some control over who that information is shared with. Connell noted that it is particularly important to allow the patient to segment data for areas in which stigma is attached and in which the patient is at risk for future violence.

Connell provided an overview of the legal protections in state and federal law regarding information about victims of domestic violence or intimate partner violence and sexual assault violence. Connell brought to the Committee's attention protocols recently promulgated by the Department of Justice, pursuant to the violence Against Women Act, regarding the sharing of

forensic record and medical records pertaining to the examinations of women who are domestic violence victims or sexual assault victims. Those protocols, which are also cited in the written testimony, underscored the need to allow the patients to impose restrictions on who gets to share that information. Connell also brought to the Committee's attention a number of provisions in state law regarding minor healthcare and the need to segregate and segment minor healthcare; it is critical that the minors be permitted a confidential opportunity to decide whether they consent to the inclusion of that information in an electronic exchange.

Dr. Gunter stated that there are enormous technical challenges with granular data sequestration. Dr. Gunter asked Connell to speak to the ILHIE implementing an incremental strategy to granular sequestration; allowing for granular sequestration as it become technically feasible.

Connell cited two White Papers that the Office of the National Coordinator commissioned from George Washington University Department of Health Care Policy, noting that both provide some guidance as to how a HIE could be set up to respect granularity.

Connell suggested a medical history report care might include data such as blood type, allergies, drug allergies, and immunizations; this limited data set could be made available to health care providers whether in an emergency situation or as a baseline for any care by a specialist or other health care provider. It was Connell's understanding that the technology does exists to segment that data and segment it either by not including it in the exchange or share the data but not have it be visible.

Dr. Gunter noted for the record two dangers to data segmentation. One of the dangers is having too high a bar, too much segmentation, that the individuals involved are disenfranchised from the system because simply no one will share any part of their record because they do not have the knowledge of tools to segment the record; this is a concern the Committee has heard repeated in testimony. The other danger is if there are a lot of vendors selling products claiming that records are being segmented. Dr. Gunter stated there needs to be some evidence that the segmentation is achieving its goals. Dr. Gunter drew a parallel to de-identification; there has been a long body of research on de-identification, the effects of de-identification and how hard that is – we need a similarly serious agenda for looking into segmentation and its effectiveness.

Connell brought to the Committee's attention the Massachusetts e-Health Collaborative, an opt-in with restrictions system noting that they have 90% patient participation. Connell shared that the e-Health Collaborative found that a meaningful informed consent dialogue does really help patients to avoid, or at least minimize confusion.

Mr. David Carvalho asked: With respect to public health, were you suggesting that current mandatory reporting requirements be revisited or that the HIE not be used as the mechanism for complying with those requirement? Or simply that those requirements currently established by law are acceptable, but public health purposes beyond thoes should not be contemplated? Connell responded that assuming that that data can be de-identified in a way that protects the confidentiality of the individual, that information might very well be included and available through the Exchange for public health and research purposes. In instances where the public health receives information in an identifiable format all patients should retain the right to decide

whether their medical information is shared.

Mr. Harry Rhodes brought to the Committee's attention that the Massachusetts e-Health Collaborative initially had a significantly lower acceptance rate of patients opting-in. The e-Health Collaborative had to retrain access clerks and registration clerks after which there was a higher response. Rhodes also brought to the Committee's attention the role, supported by numerous research studies, that health care literacy plays in patients' understanding of consent and patient choice. Providing health literacy training to the consumer has resulted in a greater patient participation. Connell concurred; to implement a system that allows for meaningful patient choice will require the intensive careful training of health care staff.

Ms. Connell's submitted written testimony can be accessed at:
http://www2.illinois.gov/gov/HIE/Documents/ACLU_CKC%20Final%20of%20ILHIE%20Testimony%207%20p.m%20July%2016.pdf

Public Comment
Mr. Bob Adams spoke on behalf of NetSmart Technologies, an EHR technology provider for behavioral health providers and public health organization. Adams provided background information on NetSmart Technologies.

NetSmart advocates the Committee undertake every possibility to include mental health and substance abuse data in the exchange of information. NetSmart clients and their patients feel they would be best served by inclusion of their data in the Illinois HIE. Adams shared that NetSmart clients see enormous benefit from participating in exchange in terms of care coordination and research to support improved health outcomes. NetSmart also supports the inclusion of behavioral health data and substance abuse data in a de-identified and aggregated fashion to support research studies.

Adams advocated in support of a uniform consent policy. Adams further recommended that in every place where the Committee is considering granularity of choice, NetSmart suggests that this Committee recommend a common uniform nomenclature, in order for the granularity of choice to be more easily executed by automated systems.

Adams indicated that NetSmart would submit a more detailed testimony and analysis to the Committee.

Mr. Adam's submitted written testimony can be accessed at:
http://www2.illinois.gov/gov/HIE/Documents/120726%20Netsmart%20Technologies%20Positions%20On%20ILHIE%20Discussion%20Topics.pdf

Lunch Break
The Committee broke for lunch at 1:00 pm.

Public Testimony – Sensitivity of Patient Data: Safeguards for Certain Personal Health Information
The Committee reconvened at 2:00pm

McGinnis read submitted written testimony on behalf of Kathy Chan of the Illinois Maternal and Child Health Coalition ("IMCHC") a statewide, nonprofit organization that focuses on the promotion and improvement of health outcomes for women, children, and their families through advocacy, education, and community empowerment.

IMCHC, in order to protect a vulnerable population, encourages the Authority to be particularly vigilant in protecting the confidentiality of minors' health records. Current Illinois state law assures minors the right to a wide variety of health services without the consent or knowledge of their parents or legal guardians. Minors' ability to access these services confidentially, and to keep their medical history private, is championed by many health professionals and advocates as essential in encouraging young people to access comprehensive health services. Parental involvement and knowledge may deter some minors from accessing the health care they require. Adolescents are simply less likely to access care without the guarantee of confidentiality. Therefore, assuring the privacy of their medical records is critically important.

IMCHC's written testimony can be accessed at:
http://www2.illinois.gov/gov/HIE/Documents/24_FINAL%20ILHIE%20testimony_IMCHC.pdf

McGinnis read an excerpt of submitted written testimony on behalf of Pamela Sutherland, Vice President of Public Policy of Planned Parenthood of Illinois ("PPIL").

Patients often have to reveal highly personal and private information when receiving medical care. The purpose of having special consent procedures for certain health services is to ensure a heightened security for that information and to assure patients that they are "safe" in revealing sensitive information to health care professionals. If patients do not feel "safe" some of them will decline health care putting themselves and possibly others at risk. Therefore, special opt-out procedures should be extended to the inclusion of personal health information related to services such as behavioral health and substance abuse. When these health services are involved, the patient should be given the opportunity to opt-out of entering that health information into the HIE or sequestering if from certain providers.

PPIL addressed the issue of minors who consent to health care services. An overview of Illinois law guaranteeing confidential care without parental consent for certain health services was provided. One of the main reasons that the law allows for minors to receive these kinds of health care without parental involvement is because there is a risk that some minors will forgo care and put themselves and possibly others at risk if parents are involved. Because minors are allowed to give consent for certain confidential health services but not all health services, the HIE must have a system set up to allow minor patients to sequester certain personal health information from both specific providers and from their parents or guardians. The minor must be able to sequester information from providers who they do not trust to keep such information confidential.

PPIL's submitted written testimony can be accessed at:
http://www2.illinois.gov/gov/HIE/Documents/PP_IHIE%20Testimony%20privacy%20security.pdf

Connell spoke to the issue of what kind of protocol might be useful in helping to segment sensitive health information. The ACLU is of the position that the Committee should recommend that protocols be developed that helps to segment sensitive patient health care information. Those protocols should include: requiring providers, prior to releasing patient names to a registry, to advise each patient individually of the opportunity to enroll in the exchange and of the right to consent to that enrollment or that general patient registry, pursuant to opt-in provisions. Patients should also be advised that they have the right to segment parts of their personal health record that the patient considers sensitive. Connell added that another really important factor is the development of protocol that allows patients to revoke consent that they've provided and that allows them to restrict the future sharing of information.

Connell discussed the issues of segmentation with respect to payers. Connell indicated her reading of the authorizing act for the ILHIE contemplates payers will have access to certain amounts of data in the system. Proceeding with that assumption, the ACLU is of the position that patients must have the ability to restrict the disclosure of PHI to payers. At a minimum, the Committee should recommend rules that are consistent with the HITECH amendments to HIPAA; allow patients to restrict disclosure to payers of personal health information that is related to treatment or services for which the patient has paid for out of pocket. A second to restriction would be those anticipated by both the Federal Genetic Information Nondiscrimination Act and the Illinois Genetic Information Privacy Act, both of which appear to allow a patient to restrict access to payers. Finally, the ACLU recommends the Committee contemplate allowing patients to restrict access to payers for all personal health information except for that medical treatment or service for which reimbursement is being sought by the particular payer seeking access to the medical care. The patient's interest in confidentiality demand that there be some time limits placed on what information payers have access to, particularly given the fact that some of those services may have been rendered years or maybe even decades before that particular payer was responsible for reimbursement.

The ACLU is of the position that consistent with existing law here in Illinois as well as Federal law, which allows patients to access their medical records that are held by individual providers, that the Committee should recommend a protocol that allows patients to both access their records through the exchange and to arrange for correction should there be inaccuracy in that record or should the record need amending.

Further, the ACLU is of the position that the Committee should consider and recommend rules that define what constitutes misuse of data that is in the exchange recognizing that the vast majority of users who access the exchange are accessing for purposes of providing quality health care and helping patients.

Ms. Connell's submitted written testimony can be accessed at:
http://www2.illinois.gov/gov/HIE/Documents/ACLU_CKC%20Final%20of%20ILHIE%20Testimony%207%20p.m%20July%2016.pdf

Public Testimony - Managing Consent

Chudzinski gave a brief presentation on managing consent. Chudzinski identified five key policy questions regarding patient choice under consideration by the Committee.

1. What is the best way to inform patient choice regarding the risks and benefits of HIEs?
2. Should providers have to discuss HIEs with patients such that "meaningful choice" is obtained? Or do "Notice of Privacy Practices" accompanied by informative website disclosures suffice?
3. Should all consents be written or can consent be obtained orally?
4. Once consent is validly obtained, is it valid for an unlimited duration of time? Or can it be revoked after a certain amount of time?
5. If consent can be revoked how should providers reconcile conflicting patient consents?

Chudzinski reviewed with the Committee OHIT's responses to recent requests for information from the Office of the National Coordinator ("ONC"). OHIT has indicated that revocation is reasonable, once validly obtained consent should be valid for an unlimited duration of time. However, OHIT has suggested that providing meaningful choice is challenging.

Chudzinski's presentation can be accessed at:
http://www2.illinois.gov/gov/HIE/Documents/Panel%205%20DPSC-7.17.12.pdf

Mr. Mike Berry spoke on behalf of HLN Consulting LLC, a health IT company on the topic of operational aspects of obtaining and managing consent in HIEs; specifically regarding different strategies in operation across the country. Berry provided some background on his engagement in HISPC and other ONC efforts related to privacy and security, including the collaboration with the Strategic Health IT Applied Research Projects on Security ("SHARPS") Program at the University of Illinois to define a technical architecture and develop a prototype for a privacy and consent layer within the ILHIE.

Berry reviewed the distinction between "push" messaging, such as Direct, in ILHIE Phase 1 and "pull" messaging, such as the aggregated query-response, in ILHIE Phase 2 noting his testimony was specific to "pull" messaging.

Berry discussed how consent model decisions impact the operational requirements for obtaining and managing consent. Berry provided several examples of operational requirements including how expected volume of consent requests and real-time consent collection mechanisms vary depending on the consent model.

Berry described the two methods by which HIEs collect consent preference from patients: directly from the patient to HIE and indirectly through the patient's provider. Berry reviewed the advantages and challenges of each approach. The primary advantages of the indirect method is that the HIE can rely on the provider to identify and authenticate the patient and that the consent action can be integrated into the patient encounter. The primary advantages of the direct method are fewer burdens on providers and potentially more control for patients. Berry stated that the challenge of the direct method is authenticating the consent; the same name matching challenges that HIE encounter when exchanging data with providers are present in accepting consent directly from patients. Berry provided a few examples of how states have operationalized the direct method of collecting patient consent. Berry reviewed several process options for operationalizing the indirect method.

Berry brought to the Committee's attention that many state HIEs have adopted incremental consent management strategies that include a less ambitious initial phase of offering granular preferences – such as an all-or-nothing consent approach, a static set of information sources and purposes of use and an unlimited duration of consent – followed by more ambitious future phase. Currently, there are few granular preferences being offered to patients in their opt-in or opt-out forms. However, many HIEs are striving to ensure meaningful choice for patients – Berry provided a few examples.

Dr. Gunter asked if there is a record of the states and the various consent options selected within those states. Berry noted that data for this testimony came from a few sources: Berry's personal experience in Vermont, Rhode Island, HISPC, the Upper Midwest State Health Policy Consortium, the ONC, and the George Washington University white papers. Aside from the ONC White Paper that had nine or ten states in it, there is no comprehensive survey of all states.

Mr. Berry's submitted written testimony can be accessed at:
http://www2.illinois.gov/gov/HIE/Documents/Berry_Testimony_2012-07-16-FINAL.pdf

Public Testimony – Identity Management

Chudzinski gave a brief presentation on identity management. Chudzinski identified four key policy questions regarding patient choice under consideration by the Committee.

1. Should the state-level ILHIE utilize a unique patient identifier for the purpose of matching patient records?
2. To what extent should the state-level ILHIE impose upon providers connected to the state-level ILHIE standards for the degree of patient matching accuracy achieved in provider systems?
3. Should patients be able to access their data transmitted through the ILHIE to check for inaccuracies?
4. If inaccuracies are apparent, should the ILHIE address patient requests to correct data or refer such requests to the patient's healthcare providers?

Mr. Chudzinski's presentation can be accessed at:
http://www2.illinois.gov/gov/HIE/Documents/Panel%206%20DPSC-7.17.12.pdf

Dr. David Stumpf spoke on behalf of Global Patient Identifiers ("GPI"). Dr. Stumpf introduced Dr. Barry Hieb, participating via telephone, an executive at GPI. Dr. Stumpf provided an overview of the current state of patient identification and the solutions necessary for accurate patient identify matching.

Dr. Stumpf noted that best of breeds systems today, using matching methods, demographics, patient identifiers, etc. are at the three sigma level. Dr. Stumpf noted that three sigma is certainly satisfactory for paying claims but in an environment where the HIE is conducting millions of transactions a day would introduce an unacceptable number of errors (misidentified patients). Dr. Stumpf advocated for identity matching at the six sigma level and based on the ASTM/ANSI standards.

Dr. Stumpf advocated for using a unique patient identifier stating that a unique identifier is crucial for managing the ambiguity of patient identification. Dr. Stumpf noted that unique identifiers could help resolve some of the issue in validating patients accessing their own records or managing consent options. Dr. Stumpf shared that the Veterans Administration has implementing a similar system that has to date saved 8 million dollars with the ability to avoid the problems of duplicate records and merged records.

Ms. Pat Merryweather noted that HIPAA included a directive to develop a unique patient identifier but that was the only item in which rules were never released due to patient privacy and confidentiality concerns. Merryweather asked what barriers still need to be overcome to implement a unique patient identifier.

Dr. Stumpf stated that HIPAA actually mandates a unique patient identifier but Congress has not allocated the funds. Dr. Stumpf suggested this opens the door to other paying mechanisms, either at the state level or through private funds. The principal reason Congress did not authorize funds was because of comments on privacy from a private community that was concerned that a patient identifier would enhance the ability to steal your identity. Dr. Stumpf stated that having a unique identifier is actually a better way to mitigate the risks of identity theft. Additionally, having a unique patient identifier helps patients identify which records and the location of those records in the event of identity theft – an otherwise difficult thing to establish without a unique identifier.

Dr. Stumpf and Dr. Hieb's submitted written testimony can be accessed at: http://www2.illinois.gov/gov/HIE/Documents/GPII%20ILHIE%20testimony%20120717.pdf

McGinnis read testimony on behalf of the Illinois State Medical Society ("ISMS").

To be successful, the HIE must ensure the secure delivery of information without placing additional administrative burdens on physicians and other providers. ISMS is concerned that federal guidance to date may add to the administrative burdens placed on health care professionals as the provisions go beyond what HIPAA require. ISMS cannot support new regulatory requirements that have the potential to place a significant administrative burden on physician practices, especially when a clear justification for the new regulations is lacking.

ISMS's concerns primarily relate to the ONC's March 23, 2012 Program Information Notice 003, which would result in additional burdensome administrative requirements placed on physician practices. It is unclear why the HIPAA Privacy and Security Rule is not sufficient to govern the transmission of patient data through an HIE. The sharing of patient records for purposes of treatment, payment, and health care operations is governed by HIPAA and this should be sufficient for HIE operations. It is unclear why the mode of secure data transmission would lead to more granular choice or why patients should be given a choice to affirmatively consent for exchange of their data through an HIE. The current security practices regarding disclosure should be sufficient for any HIE data exchange. However, if the HIE uses data beyond the treatment, payment, and health care operations exception, then it should be incumbent upon the HIE to obtain any additionally required patient consent.

ISMS expressed concerns with patient choice and consent as outlined in PIN 003, arguing that it would place undue burdens on physicians and other health professionals in an attempt to obtain "meaningful choice." ISMS stated its concerns about why the ONC would propose a standard that goes beyond HIPAA simply because protected health information data is being exchanged via an HIE. ISMS advocated that the current notice of privacy practices should be sufficient to cover data exchanges for treatment, payment, and health care operations via an HIE.

ISMS stated its option that it is the responsibility of the HIE to provide a secure environment to exchange data, and such exchange falls within the HIPAA treatment, payment, and health care operations exception. Therefore, ISMS does not see a need to collect additional consents or obtain "meaningful choice." If ONC insists on additional administrative burdens pertaining to patient consent, ISMS would suggest that any patient preferences and consent be obtained via an HIE portal. However, if a patient has restricted the release of data, such a summary of care record should be flagged to indicate that the record is incomplete so those viewing the record will know that they may not be viewing a complete record.

ISMS stated that it shares many of the same concerns expressed in the June 26, 2012 ILHIE comment letter on the Nationwide Health Information Network: Conditions for Trusted Exchange.

ISMS's submitted written testimony can be accessed at:
http://www2.illinois.gov/gov/HIE/Documents/17_ILHIE%20testimony%20pg%20-%2007%2017%2012_ISMS.pdf

Public Testimony – Security Compliance for HIEs

John Saran gave a brief presentation on security compliance for HIEs. Saran identified two key policy questions regarding security compliance under consideration by the Committee.

1. How do we foster public trust in an HIE
2. How do we protect against the misuse of data?

Saran reviewed Illinois law regarding the privacy and security enforcement providing a summary of the statute, private action to recover damages for the person affected and harmed by the crime, penalties and the agency with authority to prosecute. Saran noted the relatively small value of the penalty associated with each violation.

Saran provided an overview of the process by which the Health and Human Services Office of Civil Rights ("OCR") enforces HIPAA. Saran shared the number of breaches reported to OCR between September 2009 and April, 30, 2012 – there were 421 reports nationally involving a breach of PHI for over 500 individuals and 57,000 reports for breaches under 500 individuals. Saran noted that with limited state authority to enforce HIPAA privacy and security rules Illinois is dependent of the federal government for enforcement. Saran provided an overview of HIPAA civil and criminal violations and associated penalties.

Saran referenced new authority under the Health Information Technology and Economic and Clinical Health ("HITECH") Act that gives state attorney generals and the states authority to bring civil actions against covered entities on behalf of state residents.

Saran shared that OHIT has reviewed examples of other states sharpening their enforcing mechanisms – closing the gap between state and federal enforcement.

Saran provided a summary of the four categories of proposal to help build trust in the ILHIE under consideration: 1) monitoring and instituting monitoring systems, 2) enforcement strategies, 3) breach mitigation, and 4) public education.

With respect to monitoring Saran suggested that the Committee might recommend that ILHIE institute a breach reporting rule similar to the federal requirement. It would require all entities upon discovery of a breach to notify the state and the ILHIE. It would also allow members of the public and patients to whistle-blow on covered entities if they determine that their data has been breached. Saran suggested a technical infrastructure within the HIE to allow for real-time network monitoring of privacy and security breaches and an audit team function.

With respect to enforcement strategies, Saran suggested that the Committee might recommend that ILHIE would appoint an ILHIE Chief Privacy and Security Officer. This staff person would be charged with overseeing and managing all enforcement activities, including pursing any civil action. With respect to breach mitigation the ILHIE Chief Privacy and Security Officer would require any covered entity suffering a breach to develop a Corrective Action Plan. To address public education, it was proposed that ILHIE host a website identifying breaches and the corrective action taken, hold quarterly webinars on enforcement actions possibly requiring covered entities to participate, and/or provide grant money to non-profits to assist in a public awareness and education campaign.

Merryweather asked about enforcement policies for interstate organizations. Chudzinski indicated that there would be a role for coordinating with Illinois' counterparts from other states and with the federal government. The policy question is whether Illinois should entrust all enforcement activity only to the feds, or whether it wants to provide ILHIE and the ILHIE Chief Privacy and Security Officer additional enforcement authority.

Merryweather asked if all breaches, especially those affecting under 500 individuals require investigation to the fullest extent or is there a modified approach? Chudzinski indicated that OCR has not yet given the details of those 57,000 cases. However, from speaking to representatives of that agency, a large number of these complaints are very de minimis for example they might involve someone misdirecting a fax, and that's a reportable condition only if they're unable to retrieve or destroy that fax. There are a number of incidents that may be actual incidents but don't really affect the greater public to the extent some of these other breaches would require investigation by the Authority.

Mr. Saran's presentation can be accessed at:
http://www2.illinois.gov/gov/HIE/Documents/11d_Panels%204-7%20DPSC-7.17.12.pdf

Mr. Vik Bansal provided testimony on behalf of Deloitte on ways to better protect patient data and instill confidence in the use of the exchange. Deloitte recommended five essential elements of a successful approach to building trust: 1) implement a broad risk management program,

including periodic risk assessments and the publishing of high level results; 2) provide easy and secure information to patients about their privacy rights; 3) using role-based rules to manage data access and implement robust audit trail capabilities; 4) implementation of a consent management system that allow patients to determine view and access rights to their PHI; and 5) train employees on privacy procedures.

Deloitte advocated for OHIT to provide overall governance in establishing and enforcing security compliance standards on HIEs. Bansal suggested one possible approach for establishing security compliance standards and providing a mechanism for continuous monitoring involves using an integrated security regulatory risk framework that rationalizes industry standards, policies, and state and federal law or regulations. The security risk framework will enable OHIT to assess and prioritize security, privacy and compliance risks, then identify the appropriate risk response strategy. Bansal further indicated that the ILHIE should collaborate with sub-State HIEs to enforce security compliance standards by providing those HIEs with the necessary tools and processes to do so.

Merryweather asked whether the security risk framework was scalable; whether the approach would be applicable to small versus large organizations. Bansal responded yes, because you can rationalize different standards of regulation that may apply to one entity versus another.

Mr. Bansal's submitted written testimony can be accessed at:
http://www2.illinois.gov/gov/HIE/Documents/25_Deloitte.pdf

McGinnis read an excerpt of submitted written testimony on behalf of Pamela Sutherland, Vice President of Public Policy of Planned Parenthood of Illinois ("PPIL").

PPIL advocated that patients should be given a unique identifier. PPIL further advocated that patients should have access to their own medical records. If patients believe there is an inaccuracy, they should not be allowed to unilaterally change the data; instead, a system should be in place for the patient to contact the provider to correct the data.

PPIL advised that access to data stored in the HIE should be limited to patients and the health care professionals providing them with health care. If personal patient information is accessible to public health authorities, governmental bodies, or others, patients will not have confidence in the security and privacy of the HIE.

PPIL recommended consistency in security and privacy standards across all HIEs in Illinois to ensure that all patients are provided the same standards and to avoid patient confusion.

Public Comment
There was no additional public comment in response to the Chair's invitation.

Adjourn
The meeting was adjourned at 4:00pm. The next meeting of the Committee is scheduled for July 27, 2012.